

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

---

UNITED STATES OF AMERICA,

Plaintiff,

v.

155 VIRTUAL CURRENCY ASSETS

Defendants.

---

)  
)  
)  
)  
)  
) Civil Action No. 20-cv-2228  
)  
)  
)  
)  
)  
)

UNITED STATES’ VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW, Plaintiff the United States of America, by and through the Acting United States Attorney for the District of Columbia, and brings this Verified Complaint for Forfeiture *in Rem* against the defendant properties, namely: 155 virtual currency accounts (the “Defendant Properties”), which are further described in Attachment A. The United States alleges as follows in accordance with Rule G(2) of the Federal Rules of Civil Procedure, Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions.

**NATURE OF ACTION AND THE DEFENDANT IN REM**

1. This *in rem* forfeiture action arises out of an investigation by the Internal Revenue Service – Criminal Investigation’s Cyber Crimes Unit (“IRS-CI”), Federal Bureau of Investigation (“FBI”), and Homeland Security Investigations (“HSI”). Specifically, the United States is investigating the unlawful use of the cryptocurrency to support and finance terrorism.

2. The Defendant Properties are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as foreign assets of designated foreign terrorist organizations based in Syria that are linked to al-Qaeda, including the Al-Nusrah Front (“ANF”) and Hay’at Tahrir al-Sham (“HTS”), which have engaged in planning and perpetrating federal crimes of terrorism as defined

in 18 U.S.C. § 2332b(g)(5), against the United States, citizens or residents of the United States, and as foreign assets affording any person a source of influence over any such entity or organization.

### **JURISDICTION AND VENUE**

3. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.
4. Venue is proper pursuant to 28 U.S.C. § 1355(b)(2).

### **FACTS GIVING RISE TO FORFEITURE**

#### **I. BACKGROUND**

##### **A. al-Qaeda and Affiliated Foreign Terrorist Organizations**

5. On October 8, 1999, the United States Secretary of State designated al-Qaeda as a Foreign Terrorist Organization (“FTO”) under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist (“SDGT”) under section 1(b) of Executive Order 13224. The Secretary of State also added the following aliases to the FTO listing: “the Base,” the Islamic Army, the World Islamic Front for Jihad Against Jews and Crusaders, the Islamic Army for the Liberation of the Holy Places, the Usama Bin Laden Network, the Usama Bin Laden Organization, Islamic Salvation Foundation, and The Group for the Preservation of the Holy Sites. To date, AQ remains a designated FTO.

6. Al Qaeda’s designation as an FTO and SDGT has been renewed on multiple occasions since 1999, and al-Qaeda remains a designated FTO and SDGT today.

7. On October 15, 2004, the Secretary of State designated Jam’at al Tawhid wa’al-Jihad as an FTO under Section 219 of the Immigration and Nationality Act and as a SDGT under section 1(b) of Executive Order 13224.

8. On December 15, 2004, the Deputy Secretary of State added numerous aliases to the Jam’at al Tawhid wa’al-Jihad FTO designation including the alias al-Qaida in Iraq (“AQI”).

9. On December 11, 2012, the Secretary of State amended the FTO and SDGT designations of Jam'at al Tawhid wa'al-Jihad to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

10. On May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the FTO and SDGT designations of AQI to remove all aliases associated with ANF. Separately, the Secretary of State then designated al-Nusrah Front (ANF), also known as Jabhat al-Nusrah, also known as Jabhet al-Nusra, also known as The Victory Front, also known as Al-Nusrah Front for the People of the Levant, also known as Al-Nusrah Front in Lebanon, also known as Support Front for the People of the Levant, and also known as Jabaht al-Nusra li-Ahl al-Sham min Mujahedi al-Sham fi Sahat al-Jihadb as an FTO under Section 219 of the Immigration and Nationality Act and as a SDGT under section 1(b) of Executive Order 13224.

11. On October 19, 2016, the Secretary of State amended the FTO and SDGT designations of ANF to include the following new aliases: Jabhat Fath al Sham, also known as Jabhat Fath al-Sham, also known as Jabhat Fatah al-Sham, also known as Jabhat Fateh al-Sham, also known as Fatah al-Sham Front, also known as Fateh Al-Sham Front, also known as Conquest of the Levant Front, also known as The Front for liberation of al Sham, also known as Front for the Conquest of Syria/the Levant, also known as Front for the Liberation of the Levant, also known as Front for the Conquest of Syria.

12. On May 17, 2018, the Secretary of State amended the FTO and SDGT designations of ANF to include the following aliases: Hay'at Tahrir al-Sham, also known as Hay'et Tahrir al-Sham, also known as Hayat Tahrir al-Sham, also known as HTS, also known as Assembly for the Liberation of Syria, also known as Assembly for Liberation of the Levant, also known as

Liberation of al-Sham Commission, also known as Liberation of the Levant Organisation, also known as Tahrir al-Sham, also known as Tahrir al-Sham Hay'at.

13. To date, ANF and HTS remain designated FTOs.

**B. Bitcoin**

14. Bitcoin ("BTC") is a decentralized virtual currency, which is supported by a peer-to-peer network. All transactions are posted to a public ledger, called the Blockchain (which can be seen at <https://Blockchain.info>). Although transactions are visible on the public ledger, each transaction is only listed by a complex series of numbers that does not identify the individuals involved in the transaction. This feature makes BTC pseudonymous; however, it is possible to determine the identity of an individual involved in a BTC transaction through several different tools that are available to law enforcement. For this reason, many criminal actors who use BTC to facilitate illicit transactions online (*e.g.*, to buy and sell drugs or other illegal items or services) look for ways to make their transactions even more anonymous.

15. A BTC address is a unique token; however, BTC is designed such that one person may easily operate many BTC accounts. Like an e-mail address, a user can send and receive BTC with others by sending BTC to a BTC address. People commonly have many different BTC addresses and an individual could theoretically use a unique address for every transaction in which they engage. A BTC user can also spend from multiple BTC addresses in one transaction; however, to spend BTC held within a BTC address, the user must have a private key, which is generated when the BTC address is created and shared only with the BTC-address key's initiator. Similar to a password, a private key is shared only with the BTC-address key's initiator and ensures secured access to the BTC. Consequently, only the holder of a private key for a BTC address can spend BTC from the address. Although generally, the owners of BTC addresses are not known unless the information is made public by the owner (for example, by posting the BTC address in

an online forum or providing the BTC address to another user for a transaction), analyzing the public transactions can sometimes lead to identifying both the owner of a BTC address and any other accounts that the person or entity owns and controls.

16. BTC is often transacted using a virtual-currency exchange, which is a virtual-currency trading platform and bank. It typically allows trading between the U.S. dollar, other foreign currencies, BTC, and other digital currencies. Many virtual-currency exchanges also act like banks and store their customers' BTC. Because these exchanges act like banks, they are legally required to conduct due diligence of their customers and have anti-money laundering checks in place. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.*, and must collect identifying information of their customers and verify their clients' identities.

**B. Blockchain Analysis**

17. While the identity of the BTC address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for other currency or to use BTC to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses sophisticated, commercial services offered by several different blockchain-analysis companies to investigate BTC transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the BTC transactions. Specifically, these companies create large databases that group BTC transactions into "clusters" through analysis of data underlying BTC transactions.

18. Through numerous unrelated investigations, law enforcement has found the information provided by these companies to be reliable. The third-party blockchain-analysis software utilized in this case is an anti-money laundering software used by banks and law enforcement organizations worldwide. This third-party blockchain analysis software has supported many investigations, and been the basis for numerous search and seizure warrants, and as such, has been found to be reliable. Computer scientists have independently shown that they can use “clustering” methods to take advantage of clues in how BTC is typically aggregated or split up to identify BTC addresses and their respective account owners.

19. Since the blockchain serves as a searchable public ledger of every BTC transaction, investigators may trace transactions to BTC exchangers. Because those exchanges collect identifying information about their customers, subpoenas or other appropriate process submitted to these exchangers can, in some instances, reveal the true identity of the individual responsible for the transaction.

## **II. AL-QAEDA BTC TERROR FINANCE CAMPAIGN**

20. In April 2019, the administrator of the Telegram group “Tawheed & Jihad Media,” which is now defunct, provided a Bitcoin address starting with 37yrx7 (“**Defendant Property AQ1**”) as a repository for pro-al-Qaeda donations.

21. Posts on the Tawheed & Jihad Media Telegram group during that same time frame advertised fundraising campaigns to raise money for fighters. For example, on or about May 25, 2019, a user posted an image with the text: “FUNDRAISING CAMPAIGN” and “FINANCE BULLETS AND ROCKETS FOR THE MUJAHIDEEN.” Muhajideen in this context refers to al Qaeda fighters or soldiers. The post accompanying the image stated, “For Donations and more details: Please message: @TawheedJihadMedia.”

22. The media content of the Tawheed & Jihad Media Telegram group included watermarked images of both Ansar al-Tawheed, a jihadist group that was created in or about March 2018, and the Syria-based pro-al-Qaeda collective Wa Haredh al-Moemeneen (“Incite the Faithful”), of which Ansar al-Tawheed is a member. The collective Wa Haredh al-Moemeneen was formed in approximately the fall of 2018 to oppose negotiations with the Syrian regime and, as of May 2019, when the Telegram group administrator solicited donations to **Defendant Property AQ1**, was fighting against Syrian government forces and their allies in northern Syria.

23. On or about May 5, 2019, **Defendant Property AQ1** sent its entire balance of BTC, approximately 0.14610741 BTC, to a cluster of BTC addresses, containing the root address starting with 3LcrD (“**Defendant Property AQ2**”).

24. Al-Qaeda and affiliated terrorist groups have been operating a BTC money laundering network using Telegram channels and other social media platforms to solicit BTC donations to further their terrorist goals. As described below, al-Qaeda and affiliated terrorist groups operate a number of Telegram channels and purport to act as charities when, in fact, they are soliciting funds for the mujahedeen. Al-Qaeda and the affiliated terrorist groups are connected and use multi-layered transactions to obfuscate the movement of BTC.

25. **Defendant Property AQ2** is a central hub used to collect funds and then redistribute the funds within this money laundering network. From on or about February 25, 2019 through on or about February 5, 2020, **Defendant Property AQ2** received approximately 15.27050803 BTC via 187 transactions.

26. Between February 25 through on or about July 29, 2019, **Defendant Property AQ2** sent approximately 9.10918723 BTC via 38 transactions to an account at a virtual currency exchange (**Defendant Property 1**).

27. Funds received by **Defendant Property 1** were in turn sent to various online gift

card exchanges (“GCE”) that facilitate the sale of various gift cards in exchange for cryptocurrency. This is a common method of money laundering known to law enforcement.

28. On or about May 21, 2019, a BTC address starting with 3KhAH (**Defendant Property 2**) sent approximately 0.02825625 BTC to **Defendant Property AQ2**.

29. On or about May 29 and 30, 2019, **Defendant Property 2** sent a total of approximately 0.07640859 BTC to a BTC address starting with 3LZg4 (**Defendant Property 3**). Within hours, **Defendant Property 3** sent BTC to **Defendant Property AQ2**. This is a common method of money laundering known to law enforcement as layering.

#### **Leave an Impact Before Departure**

30. A Syria-based organization that translates to “Leave an Impact Before Departure,” has conducted donation campaigns asking people to send support via BTC. As of July 30, 2020, Leave an Impact Before Departure publicly claimed that it was a charity conducting humanitarian work. However, this group has posted images on its Telegram channel regarding the prices of military equipment needed to support the fighters inside of Syria.



31. For example:



32. As demonstrated above, these posts are seeking funds for military equipment.

33. Leave an Impact Before Departure advertised an account at a virtual currency exchange (**Defendant Property 4**) in the Telegram channel as its deposit address to which donors could send BTC.

34. **Defendant Property 4** received approximately 14.58133728 BTC via 65 transactions for the period on or about March 10 to on or about December 11, 2019. This includes seven transactions totaling approximately 0.73060999 BTC from **Defendant Property AQ2**.

35. A cluster of approximately 29 BTC addresses with a root address starting with 1JtyZ received (**Defendant Property 5 - Defendant Property 33**) approximately 0.29328346 BTC via six transactions from **Defendant Property AQ2**. Cluster 1JtyZ sent:

- a. 0.76916964 BTC via three transactions to **Defendant Property 1**; and
- b. 0.2270076 BTC via two transactions to **Defendant Property 4**.

**Al Ikhwa**

36. The Telegram channel for @Al\_ikhwa\_official appeared online in or around June 2018. The administrator of the group is listed as “@AL\_ikhwa.” The group’s profile describes them as an “independent charity on the ground in Syria” and that they “do not support any acts of terrorism;” however, blockchain analysis and a review of related social media posting demonstrates otherwise.

37. Many of Al Ikhwa’s posts on Telegram solicit donations through PayPal, Western Union and “anonymous payment” with BTC. Their first post stated, in part:

...supporting the brothers in Syria, Wives of [martyrs] and their families...[and]  
We help those who defend the Muslims in [Syria].

38. The Al Ikhwa administrator posted 11 BTC addresses for potential donors to fund (“**Al Ikhwa Cluster**”). These 11 BTC addresses represent **Defendant Property 34** through **Defendant Property 44**.

39. Blockchain analysis revealed the **Al Ikhwa Cluster** has received approximately 0.43820188 BTC via 18 transactions for the period October 15, 2018 to September 3, 2019.

40. Approximately half of the BTC received by this cluster, 0.22524884 BTC, was sent via four transfers to **Defendant Property AQ2**.

41. Shortly thereafter **Defendant Property AQ2** received BTC from the **Al Ikhwa Cluster**, the proceeds of which were sent to **Defendant Property 1**.

42. **Al Ikhwa** also operated a Facebook account which had posted four BTC addresses for donations. Two of these BTC addresses are part of the **Al Ikhwa Cluster** and the other two are part of a cluster of six BTC addresses (“**Al Ikhwa Facebook Cluster**”). These six BTC addresses represent **Defendant Property 45** through **Defendant Property 50**. **Al Ikhwa**

**Facebook Cluster** sent approximately 0.09413247 BTC during April and May 2020, via three transfers to the **Al Ikhwa Cluster**.

43. The documented practice of layering BTC transfers is observed herein, where Al Ikhwa is attempting to obfuscate the source of BTC and conceal the identity of the owner.

44. The Al Ikhwa administrator stated on Telegram:

Yeah, bitcoin makes a new one [i.e. address] every transaction so it's good, it always looks like it's going to a different place..if you ever get [a] police visit and they want to trap you to say you sent [donations] to Syria.. say they are liars..because one person told me maybe they can't track the bitcoin but they can see IP address...But our Syria IP addresses are Turkish because our Internet comes from Turkey. So if they try to trap someone and say you sent money here by showing IP address, you say they are liars and you did business in Turkey.. cause the IP address is Turkish.

45. The Al Ikhwa money laundering network conducted layered transactions including as follows:

a. **Al Ikhwa Cluster** sent 0.09019068 BTC to cluster 3HvtR on or about January 20, 2019, and then five days later this cluster sent 0.3372531 BTC to **Defendant Property 1**.

b. **Al Ikhwa Cluster** sent 0.05927279 BTC to address 36A2P on or about April 2, 2019.

i. That same day, address 36A2P sent 0.041 BTC to **Defendant Property 4**;

ii. A few days later, address 36A2P sent 0.01953034 BTC to **Defendant Property 1**;

c. **Al Ikhwa Cluster** sent a total of 0.00016023 BTC via two transactions to cluster 12Btp on or about October 19, 2018, and on or about March 2, 2019. On or about July 16, 2019, cluster 12Btp sent 0.00651841 BTC to **Defendant Property AQ2**.

**Malhama Tactical**

46. Open source reporting has linked Al Ikhwa to Malhama Tactical, a jihadist military company that trains HTS fighters and has solicited BTC to finance HTS operations in Syria.

47. Malhama Tactical is described in open source materials as a “jihadist private military company.” It is comprised of fighters from Uzbekistan and the Russian Caucasus.

48. The Twitter page of Malhama Tactical’s founding leader, Abu Salman Belarus, describes him as the “Commander of Malhama Tactical, we are the military instructors, we’ve been teaching rebels how to fight and provide emergency aid on battlefield since 2013.” In a published interview in February 2019, Abu Salman Belarus stated that Malhama Tactical worked with and trained HTS fighters. Moreover, in around July 2019, Malhama Tactical fundraised for drones to be used for “artillery adjustment and reconnaissance.” In releasing an intelligence report about that fundraising effort, the SITE Intelligence Group described Malhama Tactical as an HTS Special Forces training group.

49. Notably, an April 2020 online video from a news media outlet showed interviews with members of Malhama Tactical about certain military tactics they used after recent battles in Idlib, Syria. In a published video interview on or about June 11, 2020, a Malhama Tactical leader named Ali al-Shishani described Malhama Tactical as a group of professional instructors who trained members of the Syrian resistance and stated that HTS was one of the groups with whom Malhama Tactical worked.

50. The Twitter account of Malhama Tactical’s founder, Abu Salman Belarus, tweeted two BTC addresses when soliciting donations. His tweets stated, “You can support and help us anonymously and safely with Bitcoin wallet: 1J5x4,” and “Bitcoin wallet for support instructor team of [MT]: 1LVwt.”

51. These two Malhama Tactical addresses are part of a cluster of 23 addresses (“**MT cluster**”) that received approximately 0.19501359 BTC via 15 transactions for the period July 13 to November 22, 2019. These 23 BTC addresses represent **Defendant Property 51** through **Defendant Property 73**.

52. On or about October 9, 2018, **MT cluster** sent approximately 0.03839 BTC to cluster 3Jb1M which has sent BTC to **Defendant Property AQ2** on multiple occasions.

**Reminders From Syria**

53. The Al Ikhwa Telegram channel forwarded several posts from the “@RemindersFromSyria” (“RFS”) channel, and the RFS channel has similarly forwarded Al Ikhwa’s posts, many of which contained Al Ikhwa’s BTC addresses.

54. RFS’s channel falsely states that they are “not affiliated with any fighting groups in Syria” and they “do not promote any acts of violence and terrorism.” In fact, they have posted numerous donation requests to support foreign fighters, threats to the United States, and radical extremists abroad.

55. For example, one post showed a photograph of a machine gun with a military-style vest holding numerous additional magazines of bullets. Another post stated:



56. On or about July 16, 2020, an HSI agent acting in an undercover capacity (“UCA”) messaged the administrator of the RFS Telegram channel asking to donate BTC. The administrator provided a BTC address starting with 1CoEM (**Defendant Property 74**). Subsequently, **Defendant Property 74** clustered with **Defendant Property 75** and **Defendant Property 76** (“**RFS Cluster**”).

57. The administrator stated that he hoped for the destruction of the United States and warned the UCA to be careful of possible criminal consequences from carrying out a jihad in the United States.

58. After these illicit conversations, the administrator shared his “own wallet” BTC address starting with 1Q4xw (**Defendant Property 77**), which could be used for “jihad.”

59. The administrator complained about U.S. drones and subsequently stated that “Bullets and bombs is all affordable, but the drone stuff, its very hard to unless u have like anti aircraft stuff which is like millions of dollars. Here they shoot it with a ground to air missile.. its possible to hit them but hard. Or a 23mm machine gun. U know those big guns attached to a car..”

60. **RFS Cluster** and **Defendant Property 77** are further linked because they both, in separate transitions, sent approximately 0.003769 BTC and 0.00235163 BTC respectively, at the same time on or about July 23, 2020 to a cluster of BTC addresses with the main address starting with 3QkrD.

61. A majority of the BTC received by cluster 3QkrD is sent to a BTC address starting with 1Kszb (**Defendant Property 78**), which is hosted at the same virtual currency exchange as (**Defendant Property 1**).

62. **RFS Cluster** also sent BTC to a cluster of BTC addresses with the main address starting with 3KKa3. Like cluster 3QkrD, cluster 3KKa3 sent BTC to **Defendant Property 78** multiple times.

#### **Al Sadaqah**

63. Al Sadaqah (“charity” in Arabic) is a Syrian organization that operates social media accounts on multiple platforms which seek to finance terrorism via BTC solicitations. They described themselves as “an independent charity organization that is benefiting and providing the Mujahidin in Syria with weapons, finical [sic] aid and other projects relating to the jihad. You can donate safely and securely with Bitcoin.”

64. On its Telegram channel, Al Sadaqah openly solicited donations via BTC to an address starting with 15K9Z (**Defendant Property 79**, which clustered with **Defendant Property 80**).

65. In one such post (depicted below), they directed people to “Donate anonymously with Cryptocurrency” to **Defendant Property 79**, to support “the mujahidin in Syria with weapons, financial aid, and other projects assisting the jihad.”



66. Example posts are shown here:



**COUNT ONE – FORFEITURE**  
**(18 U.S.C. § 981(A)(1)(G)(i))**

67. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 66 above as if fully set forth herein.

68. Al-Qaeda, HTS, and ANF are designated foreign terrorist organizations.

69. The above described scheme involves these designated foreign terrorist organizations' campaigns to finance terrorism via BTC solicitations involving the Defendant Properties.

70. The Defendant Properties are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as assets of a foreign terrorist organization engaged in planning or perpetrating any federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and as assets affording any person a source of influence over any such entity or organization.



PRAYER FOR RELIEF

WHEREFORE, the United States prays that notice issue on the Defendant Properties as described above; that due notice be given to all parties to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring that the Defendant Properties be forfeited to the United States for disposition according to law; and that the United States be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: August 13, 2020  
Washington, D.C.

Respectfully submitted,

MICHAEL R. SHERWIN,  
N.Y. Bar Number 4444188  
ACTING UNITED STATES ATTORNEY

By: /s/ Zia Faruqui

ZIA M. FARUQUI, D.C. Bar No. 494990  
JESSICA BROOKS  
Assistant United States Attorneys  
Fourth Street, NW  
Washington, DC 20530  
(202) 252-7566 (main line)

and

ALEX HUGHES  
DANIELLE ROSBOROUGH, D.C. Bar No. 1016234  
Trial Attorney  
National Security Division  
United States Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, DC 20004  
Office: (202) 514-0849 (main line)

*Attorneys for the United States of America*

**VERIFICATION**

I, Christopher Janczewski, a Special Agent with the Internal Revenue Service-Criminal Investigations, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13<sup>th</sup> day of August, 2020.

/s/ Chris Janczewski  
Special Agent Chris Janczewski  
IRS-CI

I, Joseph Consavage, a Special Agent with the Homeland Security Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 13<sup>th</sup> day of August, 2020.

/s/ Joseph Consavage  
Special Agent Joseph Consavage,  
Homeland Security Investigation

**ATTACHMENT A:**

Defendant Property	BTC Address
1	1421chCK32pV32Tw5MQbiUiKWKvnmj7d91
2	3KhAHDfTuVnHUfRgQfVP4LcV8SHXpN51u7
3	3LZg4hHfbpLrJBagQqXp2agGbwrz9XpXai
4	163oWqgPk8fKhUqmHpNnoQhikfFjHyD3Pr
5	1JtyZYT4CKeKNyxMzbCpC9VJT6KTmeAKFN
6	3Bp2Eb87ApoMAsKPSQB2SAqLmRymjeLmtv
7	3HUhCkt44P3izoLZkK3rcx8NsZXKJdksh5
8	3Q4Nb6jUWAJQLq5NS7S92YPPCTcTyuSPhK
9	3Bo3cPpPjFzt6YHffRoX6ufY1b2zzVf8mT
10	3HSK6MbuowuttVBuYepEA4fyyPxHzZ6pB
11	1Awi7RLBGdT9qCo5SCB5y6Xea7MTb1F5Xc
12	33uWGWsWSTBw1KLM4UFPvxYvDJ5Xfo9s63
13	3G68RkhEDjwhajkDN83Z1611ZGnUZmvrUD
14	3QabnGEAWXrc7rvo1JcJBzUMhcifT7m6gd
15	32ZiFK53wYe5TL8zmcy7zaAvQnSd67fcA2
16	1sQ1oXjay4KwkEuVdFf7yveQFytH1ES7g
17	3PrThrqU4fhNG4LJzVT5nMDs41S7yh75Vu
18	1DnGvHRkXC7hTXuTDDxqNEwUYyhgR1nSDn
19	3J9DbduuLLU4o65Hfw29zMVoxdjKZ9CJHo
20	3MLnjFfp9VeFVQroAbENXrDyGgioT1TZJQ
21	14mNSNTp8N9ATPoyfYQCfnn8B43YjLNbwG
22	12jUCD1da5EzutFg1zWq9fhmE1dAkB5MxF
23	3Gv56YFJ5Zaue6RCDzBNFbUE7EharKXenE
24	3DJqv8q3bxSizdc47UfuGoCkAzq7QxotEV
25	35NdXGaaMV19T6yiRpNaZTN5jQiJR5F95z
26	3KiHfB5FfsEVhRowBwMDsxzT1KT9kFEsqx
27	3GfghFZjkLncctgUDdQpuZTjFHjLhH7Hn6
28	1JnweKtFaSVYZtrNs633MyAQfxv3zWybdZ
29	1PCsivNdLzKNArTewBQeXztncMRgay9A8H
30	3PZqkm88UAeYQvfgE6HnTMPgSawaLS3PCN
31	3HMhndbjj7pRc6KrxhRv9dxsGQhfA1Mae
32	39yTYpsCpfqBmpmQgZpoE4epgr7ppSDJmK
33	31xjhbbEAsC85QynVmRRnQbL5K2UgtXXhW
34	1M34CzVZEhGfLxocxFXyNSJcrxPgoEzcHH
35	1DnKvXkfAKnBnp8WzfwCFSLakoYv9y6p6S
36	1Wdq3SJiAwcW1V7wPJWvflF9ZcARXzXyz
37	161rhMMWhtFw4zSLgmubAfx9DkAnQxXLRs

38	1PQwHVZvEQM2A3vVQdsGy1PpR47fD25CBV
39	1A4kky59YcYJNThyEX9nGgj7615qnXVgea
40	1iL6WtDdonsgVsPquHDKZXScyZCWTqFnQ
41	17J9tFkU7Z5tjotQJBdsUWVxfP2WWBquyb
42	1NqrxD6SatMMu2m4vEkxfYp9UQbwrEAU5j
43	1NbsPXpCa1adNNi9fKjvTsMEWUJGWodeKc
44	1UHVEwmzVn4x6gusr9G2K6UkPN8nX8ELo
45	18HxsZy7vsYMvFMRNsbjZRQrS3A4r3YVS7
46	1MdYecvNGSwu7rTz3ACY9vdmxyQwkpVX14
47	1NhpCGz48W7T2umxZsz2XWwr8LvUEC1Rab
48	1JRXEW4qnbSbdmMq8efykq7tPaF9EH9AsJ
49	18woRRJNizuSjATH6mRwEuXChrQeJ9hzkj
50	1KPsvnx53VpJixUrdjaZtMouC7HK11qkV5
51	1LVwtwghTiorsXKtozvHHQCM3qRcse3DP
52	17qRPuXAU2yJd31e3Fdd8rWuiKUxsC85Nu
53	1JUmvgvW6A1AP2j4FG6eMgfeQi8436G9Njd
54	1BdVWKUaUkH33oB6fYs5rN6zYj4HAv9xDe
55	1Nn2jNEpE55nq66fHxbqByRnoyWgqHuF2r
56	1NR1po4isKDrTBoV2SWPt3ibNbt4kryuju
57	1Bjd913RMgMxJyqp84Uopx5GtDUYJXbcBB
58	1PYiZensBzM7Jd3YEiDYyAxagr8EFRaf8
59	1McrLZDNUEnB1i6qn25v7icCGSWi2ynamw
60	16xYb8rkWA4aaPpaqg8jsHreW64DHXUvW8
61	15kV9USE7keMUy4GBuBDXow7mydZ25RncJ
62	185i3gHsTe2kfzG6iQZGoyJX1bK4QhKHxu
63	1CxR1hxQYw953sy9nXhFKX3vQxKX2XuQNE
64	1NootiBHcBb1SrBp89uD1vV28r2bY1zjeB
65	1G3VhaP8E5CLrh1PXmbCwNgdWnYvVpSFzh
66	1B71wHvBgFqXzc3H9uxf3V1q8LB7XrdgDk
67	1CcEbXYSNwvN8T4e7rjgURATqgQEWRRqq2J
68	1BeTdU7ymcSTHfJhYKaMhJzeJMjWHEnCY
69	1BVjLitLbaHGZrfU7Xuj8js9fEPrtUGxut
70	1NjpNMuJ9BSocgibU1gCVJd3SHokSoi3sS
71	1J5x4is2cqHZFYDeaf2bih5VWVuvEcLdA
72	12eyVkVExHiBLyxoJCZfYFfo9VE5aLY1p6
73	15WezvMKGdnBjEMYjCSa3r69ZudGzGp66t
74	1CoEM6LVSxdBUiyudqLXSSuwi79j6Yb2X
75	1BpGu5BFS3uw8J81KCfvudQcHWnn95cRhQ
76	1FQkGKvP5FmYTvKP1qGG98SNVohxzzeZpQ
77	1Q4xwkF6mUGQHBUaWy2PusTJMCFZbXmwfc

78		1KszbucM4mBc6sQz4sGR2tRwc8Qn8VkCMS
79		15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpcf
80		1BQAPyku1ZibWGAgd8QePpW1vAKHowqLez
81	AQ1	37yrx7sTX3VP2BC4eKbmVZiCyH15Wavx1S
82	AQ2	3LcrDjD1AJXUk2DKshRpo7CCjMmdsWQS1R
83	AQ2	372RABNMMfY6rKEHL7k4zbGS1gdQD8fN6y
84	AQ2	37CsFAjLo4ZKdUPmj2F7TYZQFnKmQG87HS
85	AQ2	3B5p2LERKDQrBjWqaEXDXcxuXUveqRAcWd
86	AQ2	3QadnFouUe4iDiCyC4ETjFawf7ec6XeT4S
87	AQ2	bc1q84ue52z2p6mxz7080f5wcf4hfmDscvng8kydr
88	AQ2	36g1AzDkxFfmUBtBvShW9BE4qoCYwtYHE
89	AQ2	3DaEFm23S1scNf63xYJGmhNLHs9nnGNAQp
90	AQ2	331AkqgXeLxAZ9WcmEha3hBbFcJduTeqPf
91	AQ2	bc1qtpdhcm5rx8e58aj6les0e2aqfddtf7s2zyfl
92	AQ2	3MCA9HSAKNDJm7VToyvXmjR7nE9XEbj5W9
93	AQ2	1AyBtxgmP1MWxMSokB36t6BvAScRQWPfUY
94	AQ2	1C7rUNar8G8v5vWAqg1FkidJAj9PdAaqNq
95	AQ2	34JUtdmLkd1LkZ1eSKJ2KpRqMhSt4fNAXA
96	AQ2	3EbW7JkomWTuhMtMAv4i7bNSCEoRPktGd7
97	AQ2	3EYRY54QutwDZcUANB3RiUD1vpFYAY43Qx
98	AQ2	3FQgB6DMBeWZ7wgJCJ8NLBh7rWs4QLPPYX
99	AQ2	3LbjnkMzHBrhyn5UX6vUVzqqCbZMqhipcA
100	AQ2	1L9H7gdwyCsUk1hG2QPA2KyPKD6BWXmzXh
101	AQ2	1DzHmgAJawvA8ZawUmsxKfN1qcDHvC8JGU
102	AQ2	3L6h9mKJcmd4hn4NpZi1RdKCrs7q2AFQct
103	AQ2	3GVbjrZD8mAmH71QqPuKimPaBnNTopQv9M
104	AQ2	1NbvLuxxBtM6M21i3pNNwjtE669s1kFaPv
105	AQ2	33yRKW3uquTTiveVb9EGb7sywXD8yiEXVj
106	AQ2	35Y4ET8Lp4G4MCefPhpRTJKACe15TvEsJo
107	AQ2	3Ln5VWAfn5VfyLLhgaz7QtFPRsaz71CaJY
108	AQ2	3ErJ9qAxB6zz3wuowu9K2bdRS6ZjkE7cC8
109	AQ2	1HMDogpJTdJNKwEwnBtrP9NEQduZ351CNK
110	AQ2	3GbTitJyBLgo7oVKA6NCKa5aq7xZBNMCvG
111	AQ2	1CwVW45KkWjFeBoP1LZSESNnh8vQR2g7bG
112	AQ2	1EPnWUooTb4Cz9WpnxidRotevaZFUFfiVG
113	AQ2	1NTdgFn7q1mAtpGWzunaYgoMRriNdupfmm
114	AQ2	1KY3mPxaB4KYKhiGoJsDXYtgkQPouVn8kr
115	AQ2	18Woupz3chLHCdbjXeJWXEi7FJpYLGtpFh
116	AQ2	3DFgq7WR8ng4mQx4kTqNm1YcMokmz5H71P
117	AQ2	391TpBcg9SzwUHWK8cSAXoaMilKkvxri3F

118	AQ2	1FbxH4UnNXXx2yMrDH9JM1nTK2uRK7tbbm
119	AQ2	1tKfLT8tL8APBDk4cS929EZ7ZnKLgYF2R
120	AQ2	34FTVSKVhTs5nnbgMyCPpdUXAA2tMnTiHZ
121	AQ2	1Pe3Emzjrhoqz5odkZRFU1Zf6qPiDaQgxP
122	AQ2	3FtCpM8a2bpTziAozbC1wHyJJ8Mf8vhHCf
123	AQ2	33868RXegKD9KJwWGNjDGhpve3SZCWtvFK
124	AQ2	3HaZrRZsepCeSWHpVkywT5ZxTuj3rgq6vb
125	AQ2	36nvxwHtFEfETZN61z7Fxm7rmaXTSohrK3
126	AQ2	3FLvM3FLahm1Cg44beb1UeLxD1a8RZDzT5
127	AQ2	3MyxLuH79hFjJv5txfZky2m1QUXnyKedfP
128	AQ2	3CKqK7TaY11Hvo7JfnPMhAXGVj9hZnmYjw
129	AQ2	3JAz5syB4JbkpC3s5gykNeRY21rChPp14
130	AQ2	35bTbKarTJoXX2N3qjz9WpECGzJG23gBsV
131	AQ2	33z7aAa52fwnxEi3MJ2kCSytipC7nwrRj
132	AQ2	3LMnbGBJe6ZUtCarGgRhKuAXmiVkYf6WZj
133	AQ2	3M3QCf2euKqJhPEbni5bXh675pUkU3x4zC
134	AQ2	3KSuGp6RQbrFAugje78qiqkUZ4rSFoUTvK
135	AQ2	3Fij9xVYCdn9h8CdjaJBzdW7dmU8aHzWLf
136	AQ2	3N9vcfrAohotVCNJzQx2srHf69viMHhrqX
137	AQ2	3G7CuBeXcFrSyB2fkx2GvfBDYoUD2oghxR
138	AQ2	3LpaQzZUPFeR2LF55sumb9kZk4j5HdMUaC
139	AQ2	3FDNrcgT6hV8swepYLPFCALy4oZMqyxKFU
140	AQ2	3F4GniWYtwU6W1bMV432DE1Q1P9qcDHCfI
141	AQ2	3Md8xo8ug4Rm1WSLWjK3NUDaFBpyHm4hEp
142	AQ2	35tGYGmcq7Hj2M6GTDxbCYaK1Dw98xBRST
143	AQ2	3Dbv6vnbRsF9Kiqc8er2ykmSwd2g828D6F
144	AQ2	36o6t4aXtjGV8hx1Qwg6XAQ1jeUYFxFUGuz
145	AQ2	3ErTJgH6QnYeUcbVq79gTmYsepapbRxiAE
146	AQ2	33VPbqSAH86mMzz8UpjZ5cJBCpMB3iCwSs
147	AQ2	3DQu9fGbsbyH5f5FeY4YmtsMHqWU7EJWGZ
148	AQ2	36DfazzthtbdpWg23bKTDh54vapjYN5ACM
149	AQ2	32nDFPvVHU3gYaB7JzduMjLGb4Vxw9JeEY
150	AQ2	3Qep64j3PbVow66j4KzB5KhwKXGmkLTc7Z
151	AQ2	395JzR5iGTFq9Qrw4iDrECtrHXGcz2wqQv
152	AQ2	1LAS42uBuCD7tpUR9RPyM61TnMee5y7aYw
153	AQ2	37qXWELabpGQZ7pich2qxZNveEMT7iYxNf
154	AQ2	1AmYvWtDbxgU2eYxEfdQRicj4hBr3k4wtv
155	AQ2	1DTzYoa85xFfKcYK4iqSfbkFHhaeZhXpA3